Lloyd's Register Foundation

The Alan Turing Institute

Insight report on distributed ledger technologies

Safety of engineered systems

September 2017

Lloyd's Register Foundation
Report Series: No. 2017.4

About the Lloyd's Register Foundation

The Lloyd's Register Foundation is a charity that helps to protect life and property and support education, engineering-related research and public engagement.

Our vision is to be known worldwide as a leading supporter of research, training and education – relevant to the field of engineering – which makes a real difference in improving the safety of the critical infrastructure that is vital to modern society. To support this, we promote scientific excellence and act as a catalyst working with others to achieve maximum impact.

www.lrfoundation.org.uk

About The Alan Turing Institute

The Alan Turing Institute is the UK's national institute for data science. Our mission is to make great leaps in data science research in order to change the world for the better. We work with partners in industry, public sector and third sector to drive real-world impact and pioneer the emerging discipline of data science, training the next generation and shaping the public conversation.

www.turing.ac.uk/data-centric-engineering

The Lloyd's Register Foundation report series

The aim of this report series is to openly disseminate information about the work that is being supported by the Lloyd's Register Foundation. It is hoped that these reports will provide insights for the research community and also inform wider debate in society about the engineering safety-related challenges being investigated by the Foundation.

Lloyd's Register Foundation is a Registered Charity (Reg. no. 1145988) and limited company (Reg. no. 7905861) registered in England and Wales, and owner of Lloyd's Register Group Limited.
Registered office: 71 Fenchurch Street, London EC3M 4BS, UK

T +44 20 7709 9166
E info@lrfoundation.org.uk

Contents

Executive summary

Distributed ledgers are a special type of database whose contents are distributed across a network in multiple sites, countries or institutions and use cryptographic techniques to provide a transparent and permanent record of activities between parties within that network. They present an opportunity for extraordinary innovation in meeting the challenges of providing assurance and safety of engineered systems.

Digitalisation is having a profound effect on society as we seek to improve performance, efficiency, safety, and reliability in our everyday activities. In engineering, digital technologies are supporting more widespread adoption of advanced manufacturing processes, providing additional product functionality, shortening product lifecycles and allowing more flexible use of the most appropriate resources, often leading to more complex and widely distributed supply chains.

But while such technologies are transforming how we live, their rapid adoption has left a number of challenges that must be addressed. The shortening of product lifecycles has resulted in dramatic increases in waste and difficulties in managing it. This waste is often transported for disposal or recycling to less well developed areas of the world where lack of controls can lead to health hazards for the population. Complex supply chains are difficult to manage with an increased potential for counterfeit goods to enter the supply chain, as reported by bodies such as Europol, with detrimental effects on product safety or environmental impact.

As highlighted in Lloyd's Register Foundation's Foresight review on big data, an increasing reliance on data within engineering also presents challenges. Many engineered systems rely on data for their safe and reliable operation, from aircraft and motor vehicles, to rail networks and other critical infrastructure; the development of smart factories and autonomous systems will only serve to increase this reliance. Digitalisation in engineering lifecycle processes means that risks must be managed in both the physical and digital domains. Issues such as data theft and corruption or falsification of sensor data or its resulting information present serious threats to the dependability and

Distributed ledger and blockchain technologies present an opportunity for extraordinary innovation in meeting the challenges of providing assurance and safety of engineered systems.

safety of engineered systems. Furthermore, in the continued drive to improve efficiencies and drive out costs of through-life ownership, practices such as predictive health monitoring of an asset, that rely heavily on data, will become more widespread and an understanding of the asset's origin and analysis is key in obtaining an accurate understanding of its 'state'.

Growing interest in the use of distributed ledgers and blockchain to store, process and assure such data is resulting in an increasing level of investment. The first real application of blockchain technology was in the cryptocurrency Bitcoin that some believe will cause significant changes in the financial services sector. This family of technologies has the potential to bring about such changes in a much broader range of industries, especially where there is still significant scope for digitalisation and automation of processes. The family's potential ability to provide a technological solution to lowering uncertainty between people and/or organisations means that the technologies may have a role in addressing unsolved challenges such as the threats of counterfeiting or falsification of logs.

This report aims to provide a greater understanding of distributed ledgers and blockchain technologies and their underlying concepts in order to provide more clarity on the applications in which they might be used, with a specific focus on engineered systems. Several distributed ledger systems with differing design philosophies are described in order to demonstrate the range of capabilities of such technologies.

Applications of distributed ledger and blockchain technologies within engineered systems are explored on the basis of literature research, interviews with experts and a workshop which brought together representatives from across a range of industry sectors, academia and government. The report also looks at the challenges that need to be considered in any potential implementation, or that might hinder more widespread adoption.

The report concludes that distributed ledger and blockchain technologies have a potentially wide range of applications related to engineered systems, particularly where a permanent and auditable record of activities is required. Examples already at various stages of development include the tracking of food products through a supply chain to provide transparency of their provenance and the verification of shipping container mass to avoid misloading of ships. Such examples demonstrate the scalability of the technology to applications, for instance, in assuring the provenance of engineering system components.

Key challenges associated with the technology itself are also described such as its scalability and interoperability with existing systems. Examples of work being undertaken to address these challenges are given and recommendations are made for further work to be conducted, such as the development of training and technology maturity levels, and road mapping.

Foreword

Lloyd's Register was the world's first classification society and has provided asset assurance services for over 250 years. The original aim was to provide transparency of information to merchants and underwriters on the quality of their vessels and this was recorded in the Register. The need for transparent and auditable records remains a fundamental aspect of ensuring the safety of engineered systems today and new technologies are offering solutions that should be explored.

The need for transparent and auditable records remains a fundamental aspect of ensuring the safety of engineered systems today and new technologies are offering solutions that should be explored.

Distributed ledgers are types of database whose contents are distributed over multiple locations. Using cryptographic techniques, they are able to provide a transparent and permanent record of activities, capabilities that echo the original activities of Lloyd's Register.

But how could they be more widely used to improve safety and do they have other characteristics that could provide wider benefits within engineered systems in society?

Lloyd's Register Foundation is working in partnership with The Alan Turing Institute to support data-centric engineering. This has at its heart the need to responsibly handle decentralised data assets. We are committed to catalysing and supporting innovative ideas that support the safety and reliability of engineered systems and will constantly engage in horizon scanning to anticipate developments that could dramatically change how computing and data analytics is performed in the future.

As part of this work we commissioned this insight report to help improve the understanding of distributed ledgers and blockchains. The report looks at how they might be used beyond current applications in financial services and explores their potential uses to improve the safety of engineered systems.

Professor Richard Clegg
Foundation Chief Executive
Lloyd's Register Foundation

Professor Mark Girolami
Director for the Turing-Lloyd's Register Foundation
Data-Centric Engineering Programme

Background

This report has been commissioned by the Lloyd's Register Foundation and The Alan Turing Institute through the Foundation funded Data-Centric Engineering Programme. It provides insight into distributed ledger and blockchain technologies in the context of how they might be used to help address the challenges associated with improving performance and safety of engineered systems.

Lloyd's Register Foundation is a charity and owner of Lloyd's Register Group Limited (LR). LR is a 257 year old organisation providing independent assurance and expert advice to companies operating high-risk, capitally intensive assets primarily in the energy, maritime and transportation sectors. It also serves a wide range of sectors with distributed assets and complex supply chains such as the food, healthcare, automotive and manufacturing sectors.

The Alan Turing Institute is the UK's national institute for data science, founded in 2015 by five universities (Cambridge, Edinburgh, Oxford, Warwick and UCL) and the Engineering and Physical Sciences Research Council (EPSRC). Its mission is to make great leaps in data science research in order to change the world for the better. It works with partners in industry, public sector and third sector to drive real-world impact and pioneer the emerging discipline of data science, training the next generation and shaping the public conversation.

This report is the output from research conducted across disciplines and industry sectors related to the Foundation's mission. A core input to this was a workshop held at The Alan Turing Institute in January 2017. Participants, who made a valuable contribution to this report, comprised representatives from international government bodies, industry, academia and professional representative bodies. A number of the representatives were specifically involved in the research, development or deployment of distributed ledger technologies; others were professionals within relevant industry sectors.

Building on the findings of this report, the Lloyd's Register Foundation and The Alan Turing Institute will look to identify areas of distributed ledger and blockchain technologies where further research and development will help to make a distinctive and positive impact in key areas of engineering.

Author and contributors

Principal author

Gary Pogson
Lloyd's Register and The Alan Turing Institute

Contributors to the report

Sundeep Bhandari
National Physical Laboratory

Dr Ruth Boumphrey
Lloyd's Register Foundation

Professor Matthew Chalmers
University of Glasgow

Jody Cleworth
Marine Transport International UK Ltd

Professor Graham Cormode
University of Warwick and The Alan Turing Institute

Alpesh Doshi
Fintricity

Vincent Doumeizel
Lloyd's Register

Dr Gideon Greenspan
Coin Sciences Ltd

Darren Grey
The Alan Turing Institute

Dr Shahid Hanif
The Association of the British Pharmaceutical Industry

Kevin How
Lloyd's Register

Professor Aggelos Kiayias
University of Edinburgh

Benjamin Koppelman
The Royal Society

Ahmed Kotb
The Institution of Engineering and Technology

Ben Laurie
Deepmind

Professor Vili Lehdonvirta
Oxford Internet Institute and The Alan Turing Institute

Dr Leon Lobo
National Physical Laboratory

Tim McGarr
British Standards Institution

Mike Ormond
Microsoft

Tom Price
HM Treasury, UK government

Dr Jan Przydatek
Lloyd's Register Foundation

Lady San Pedro
Project Provenance Ltd

Dr Jatinder Singh
University of Cambridge

Thomas Smart
Lloyd's Register

Professor Chris Speed
University of Edinburgh

Dr Ben Tagger
UK's Government Office for Science and The Alan Turing Institute

Dr Philippa Westbury
Royal Academy of Engineering

Alexander Woods
Chartered Quality Institute

The author wishes to acknowledge the support from other individuals and organisations who joined the workshop and were involved in carrying out the research for this work.

Does distributed ledger technology matter for engineering?

Distributed ledger and blockchain technologies are recent innovations in computer science and pervade news articles, internet blogs and social media. They are special types of database, typically spread over multiple locations, that can provide an auditable and cryptographically secure, permanent record of activities or transactions conducted across a network.

A broad cross section of the business community from new start-ups to major multinationals is investing heavily to determine what this family of technologies can do to address their challenges. Governments too have recognised the potential for the technology; the UK Government Chief Scientific Adviser (GCSA) highlighted potential opportunities within the field of forensic science for assuring authenticity and provenance of people and things in the GCSA Annual Report of 2015[1]. The UK government's vision for blockchain and distributed ledger technologies was further expanded in a GCSA Blackett Review[2] published in January 2016.

The range of potential applications being considered for these technologies is vast, with many believing that a core capability is in providing a technological solution to addressing uncertainty and trust between two or more people, organisations or nations. To date, the majority of applications have been finance (Fintech) focused which is perhaps not surprising when blockchain is one of the key technologies that underpin the Bitcoin cryptocurrency[3]. While applications outside Fintech are beginning to grow, the number of mature applications is relatively small and good technical understanding, or even knowledge of its existence, is quite limited.

'Engineering is about the practical delivery of scientifically informed solutions for the great challenges and opportunities in a rapidly evolving world.'[4] The Lloyd's Register Foundation and The Alan Turing Institute ask whether distributed ledger and blockchain technologies might offer solutions to the evolving challenges of providing assurance and safety of engineered systems.

Could distributed ledger and blockchain technologies offer solutions to the evolving challenges of providing assurance and safety of engineered systems?

In order to explore this question in more detail, this report sets out to answer the following key questions:

- Within the industry sectors related to the Lloyd's Register Foundation mission, what are the challenges that distributed ledger and blockchain technologies might help to address?
- What are the key characteristics of distributed ledger and blockchain technologies that might make them an appropriate solution to the identified engineering challenges?
- What are the inherent challenges associated with using these technologies that need to be overcome?

The engineering challenges

Data is a key asset for society and particularly within engineering processes. The modern world relies on data for a wide range of engineering activities, from designing and building transport systems and critical infrastructure, to the development of pharmaceuticals, and the management of product supply chains. Mass production and dramatic improvements in product quality would likely not have been possible without the collection and analysis of large amounts of data.

For the purposes of this report, the real value of data comes from its impact on the dependability and safety of engineered systems. Already, data and information are integrated components of engineering lifecycle processes and, as assets become increasingly 'data-enabled' and interconnected, the opportunities for innovation in improving performance and safety become ever greater[5].

However, while digitalisation has been shown to bring about many advantages, it has also led to new types of vulnerability with risks needing to be managed in both the physical and digital domains. The types and extent of such vulnerabilities have been highlighted by recent high profile examples of hacking, involving the stealing of private information or the remote installation of malware to cause denial of service in critical infrastructure.

As more goods and services are represented and traded in the digital domain, careful consideration needs to be given to the mechanisms through which their quality and integrity is achieved, for example, to protect against counterfeit items entering the market which can have potentially serious safety and environmental consequences. A report commissioned by the International Chamber of Commerce in 2016[6] estimates that the economic value of counterfeit and pirated products for 2022 to be between $1.9 trillion to $2.8 trillion.

In general, the engineering challenges considered within this report fall under four categories[7]:

- Information theft
  - Personal and corporate data (for example, design information), eavesdropping
  - Asset utilisation and performance (space and time patterns)
- Disruption or prevention of asset operation
  - Hacking of control networks to disrupt or prevent asset operation (for example, denial of a physical service, like air-conditioning for server rooms)
- Corruption and falsification of sensor data
  - Energy theft (for example, by hacking smart meters)
  - Spoofing management systems (for example, buildings and transport systems)
- Falsification of information
  - Supply chain issues (third party assurance, responsiveness of actors, trust in actors, for example, suppliers)
  - Product provenance issues (for example, pharmaceuticals, aerospace and marine equipment spares). Challenges for auditing due to lack of transparency and limited oversight, that is to say, gaps in assurance activities.

A summary of where distributed ledger and blockchain technologies are considered to be potential solutions for specific sector challenges is provided in table 3 later in the report (see page 29).

What are distributed ledger and blockchain technologies?

If the full potential of these technologies is to be understood by engineering communities, it is necessary to provide a greater comprehension of their range of capabilities, what the limitations and challenges to implementation are, and what further work needs to be undertaken to facilitate wider adoption.

In this respect, the first concept that must be understood is that distributed ledgers and blockchain are not two separate technologies; they are part of a family of technologies. Each variation or member of the family, and there are many, might be considered as a system, and each of those systems is comprised of sub-systems or components that might be assembled in different ways to meet a particular need. Some systems, such as Ethereum or Hyperledger, have been designed to have multiple applications, as their developers envisaged they might be used, for example, to provide traceability in supply chains or for providing digital identification of people or products. There are many systems, such as Bitcoin, which are intended specifically to be used as a currency (often referred to as a cryptocurrency), and there are some designed for other very specific purposes, such as Corda, whose key purpose is to record, manage and synchronise financial agreements between regulated financial institutions. These specific examples will be explored in more detail in the next section, page 15.

One of the key barriers to understanding is the often inconsistent use of terminology. 'Distributed ledger technologies' is a term that is generally recognised to describe the family of technologies, while the term 'blockchain' is often used to refer to specific types of distributed ledger. Currently one person or organisation's view of what the term 'blockchain' means can differ from another. It is therefore important to define the terms and explain why variation in the meaning might be expected.

It should be noted that an International Organization for Standardization (ISO) committee is engaged in examining standardisation issues for distributed ledger and blockchain technologies, with terminology being identified as a priority at the inaugural meeting. Recognising that the formal definitions are under development, the following terms are provided for the purposes of this report. As 'distributed ledger technology' (DLT) and 'blockchain' are often used interchangeably, unless a specific type of the technology is being referred to, the term 'DLT/blockchain' will be used[8].

Ledger
A 'book' in which things are regularly recorded, especially business activities and money received or paid[9]. For the purposes of this report, this may also refer to an electronic record.

Distributed ledger
Distributed ledgers are a special type of database whose contents are distributed across a network in multiple sites, countries or institutions and use cryptographic techniques to provide a transparent and permanent record (ledger) of activities (transactions) between parties within that network. An example of a distributed ledger is R3's Corda[10].

Note: Distributed ledgers may sometimes be referred to as special types of distributed database. Additionally, not all distributed ledgers are blockchains.

Sub-categories of distributed ledger and blockchain
Distributed ledgers and blockchains are typically subcategorised as follows[11]:

Public

- Anyone in the world can read the contents.
- Anyone in the world can send transactions to and expect to see them included if they are valid.
- Anyone in the world can participate in the consensus process – the process for determining what blocks get added to the chain and what the current state is.

Private

- Permissions and rules controlled by third party.
- Transparency may be restricted.
- Participants typically known to each other.
- Resource intensive consensus mechanism not required.

Consortium

- Openness defined by the consortium.
- Consensus controlled by pre-selected set of nodes, for example, a consortium of 10 organisations requires a specific sub-set of nodes to validate a block that may or may not evolve over time.
- Contents could be public or only available to consortium.
- May make use of a public blockchain.

Distributed database
A collection of software that allows several databases to operate as though they were part of a single logical database, even though they are actually separate and possibly deployed at different sites[12]. Many distributed databases are managed by a central party but nevertheless require consensus on applying a transaction through use of algorithms. Examples of distributed databases include Apache Cassandra and Google BigTable.

Blockchain(s)
Blockchain(s) is a term typically associated with a special type of distributed ledger that may be other instances or forks of the same technology that underpins Bitcoin, or has similar characteristics. An example of such a system is Ethereum. A key characteristic of blockchains is that they use a data structure where transactions are organised within a block, and each block is 'chained' to the previous block using a cryptographic hash function.

Some experts express the view that the key innovative aspects of blockchain only exist where the system exhibits the characteristics shown for public distributed ledgers. Nevertheless, systems have been developed that are referred to as blockchain but with access permissioned through a central party. Such systems are focused towards enterprise applications and are often referred to as blockchain because they use chained-block data structures. In evaluating whether to employ such platforms, the system designer would need to carefully consider the specific benefits as compared to other types of database.

'The' Blockchain

'The' Blockchain commonly refers to the specific distributed and decentralised public ledger in which all Bitcoin transactions are recorded[13].

Type of system	Examples
Distributed database	Apache Cassandra Google BigTable
Distributed ledger	Corda
Blockchain	Bitcoin Ethereum

Table 1: System examples within the family of distributed ledger and blockchain technologies

From public to private: types of distributed ledger technologies

Having defined the terms, the most effective way of providing an understanding of the capabilities of the technology, and therefore what it can and cannot do in the context of engineering challenges, is to describe some real world examples. An understanding of key characteristics, such as the range of potential options for governance of a system, is essential to developing an understanding of where a specific type of system is suited to addressing a specific engineering challenge.

In this section four contrasting examples of distributed ledgers are explained. At one end of the spectrum the example centres on permissionless blockchain architecture, Bitcoin, while at the other is a fully private, non-blockchain distributed ledger, Corda.

The key components that form such systems can be assembled to provide alternative system architectures that suit the needs of specific applications and examples such as Multichain by Coin Sciences[14], MAS Protocol by Agility Sciences[15] and Verifiable Data Audit by DeepMind Health[16] are being launched on a regular basis. In referencing the underlying system components, an overview of the history of such technologies can be obtained together with an appreciation of how they might evolve in the future.

The Bitcoin Blockchain

Examples of distributed ledgers would be incomplete without providing an explanation of Bitcoin and its underlying blockchain technology.

Bitcoin is a distributed, peer-to-peer electronic cash system, or cryptocurrency. The specific solution conceived by Satoshi Nakamoto had the following aims:

- To allow anybody to use the system without the need for a trusted central authority.
- To make it computationally impractical to reverse transactions.
- To prevent double spending of the same 'coin'.

Transactions

Transactions are one of the key elements to understand in Bitcoin; transactions demonstrate that the owner of some bitcoin has authorised the transfer of some of it to another owner. An owner of the coin is required to digitally sign the transaction and as this process continues, a chain of digital signatures is formed, which is how Bitcoin's electronic coin is defined[3]. An outline of the lifecycle of a transaction within Bitcoin is shown in figure 1.

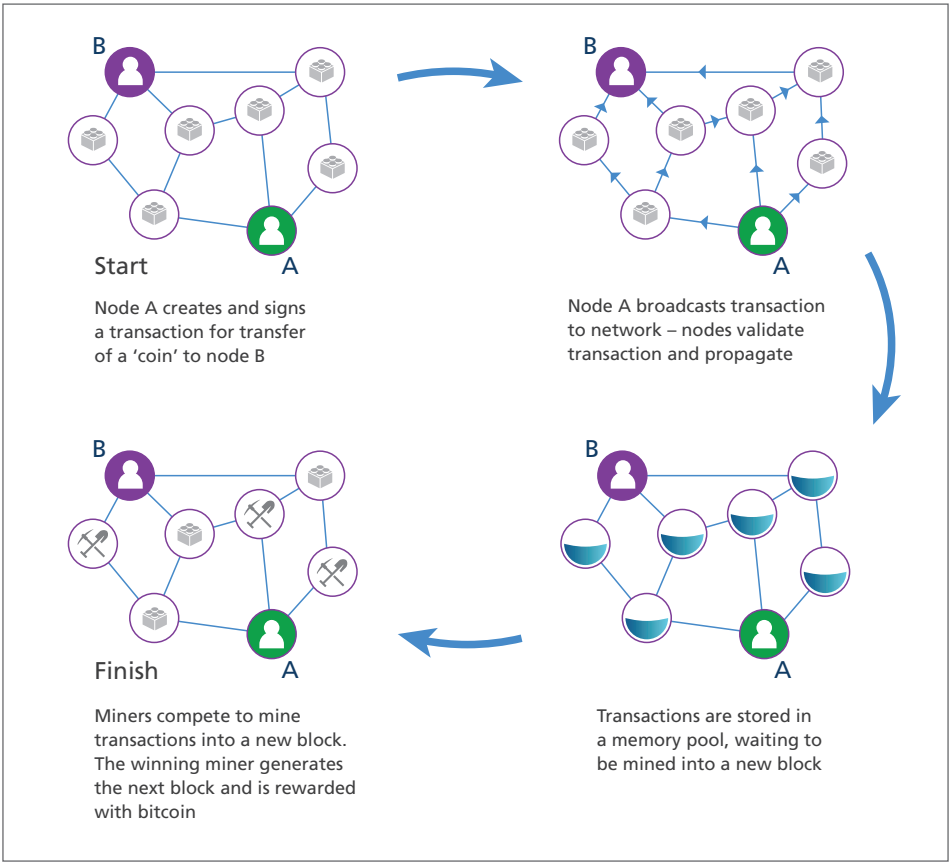

Figure 1: The Bitcoin transaction lifecycle

Mining

Mining is one of the key innovations of Bitcoin. Its principal function is to secure the system against fraudulent transactions, for example trying to spend the same bitcoin more than once. It is also how a new bitcoin is added to the system and it forms part of the process for achieving consensus on validity of transactions within the network, namely, all nodes having the same agreed version of the ledger.

The term mining is associated with the mechanism for generating new bitcoin but, just as with physical mining, resources must be expended to obtain it. In the case of Bitcoin, the resource is electricity and computer processing which is being used to solve a mathematical problem set by the system. The solution to the problem is a cryptographic hash value that has a specific number of leading zeros set by the system. The hash value is generated from inputs associated with the block as shown in figure 2.

If the hash value generated during a single iteration does not have the requisite number of leading zeros, the mining node will continue to iterate using a number known as a nonce until it achieves the target or some other node gets there first. The hash that meets the target is known as the proof of work - it proves the node has expended processing power as per the rules of the system to solve the mathematical problem. The difficulty of the mathematical problem is dynamically adjusted by the system to maintain a block generation rate of approximately one every 10 minutes. The reason why nodes are asked to expend electricity on an otherwise meaningless problem is that this safeguards against a Sybil attack*, where an adversary sets up a large number of nodes to attempt to get the network to validate fraudulent transactions.

Hash functions

A (cryptographic) hash function H, is a function that takes any input (a message) and converts it to a fixed length output, for example 256-bit, to produce a 'message digest'. Hash functions are designed to make it computationally infeasible to find a message that corresponds to a given message digest. Any changes to a message will, with a very high probability, result in a different message digest.

Typical hash functions are the SHA-1 (Secure Hash Algorithm-1) and the SHA-2 family of algorithms, for example, SHA-256. They are defined in two Federal Information Processing Standards that have been developed by the US federal government for use in computer systems by non-military government agencies and government contractors.

A representation of the creation of a bitcoin block hash is shown in figure 2.

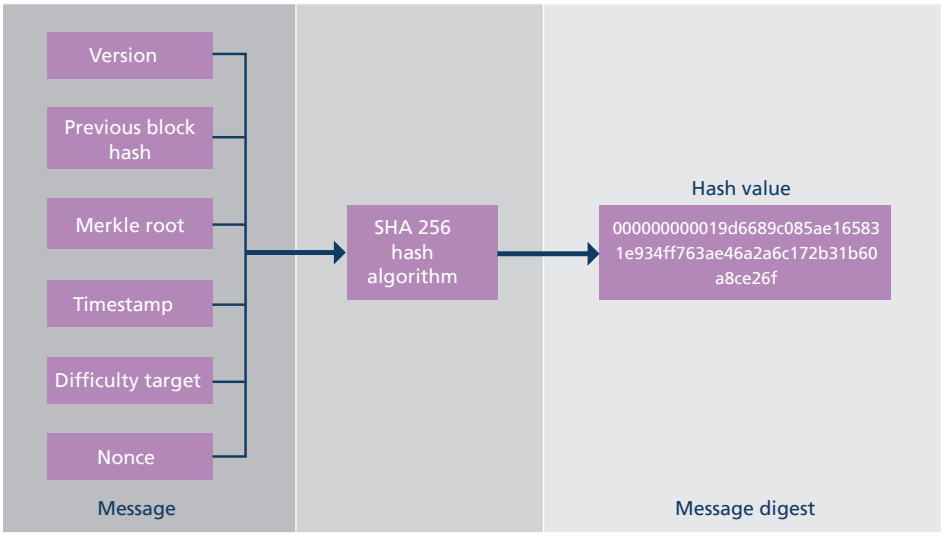

Figure 2: Creation of a bitcoin block hash value

* See glossary page 51.

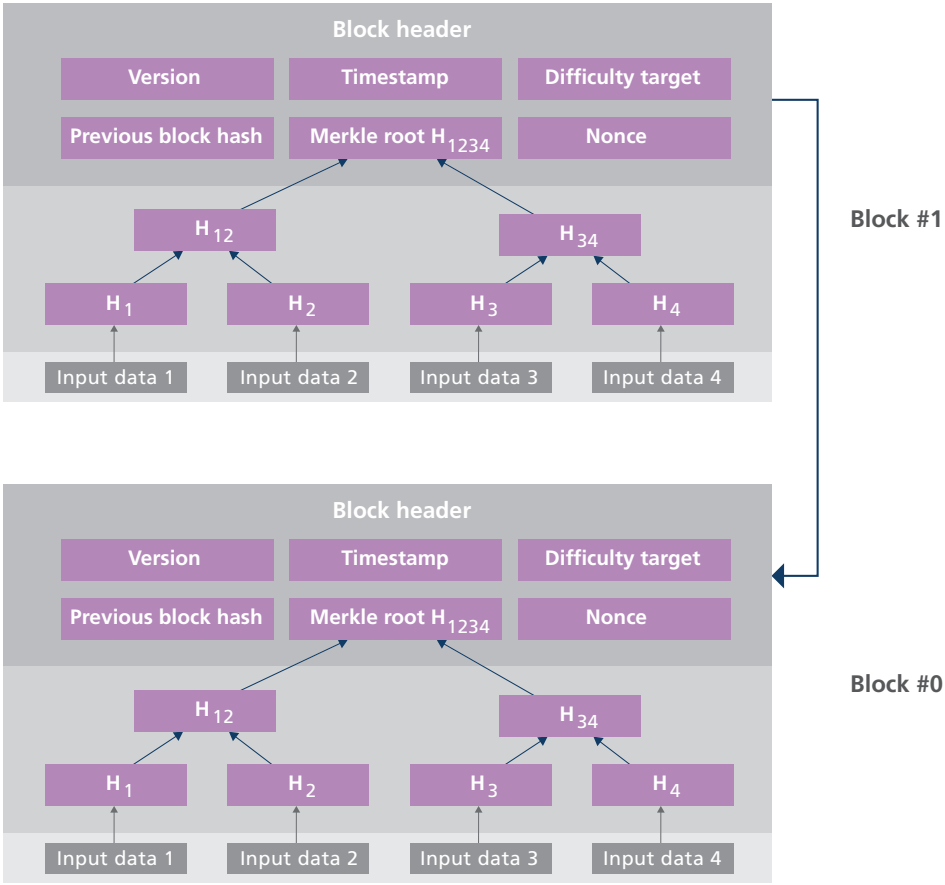

Figure 3: Representation of a blockchain

Blocks and the blockchain

The blocks in the blockchain are data structures typically represented as shown in figure 3. They are linked to form the blockchain by cross-referencing a cryptographic hash of the previous block. This reference provides for traceability all the way back to the first block created which is known as the genesis block.

This hash link between blocks ensures the append-only characteristic of the ledger because if a user tries to add or remove a transaction, or change an existing transaction, it will affect all the following blocks. Provided the latest hash is being monitored by the network any attempt to subvert the system in this manner will be obvious.

There are typically more than 500 transactions within a block and, to improve efficiency, they are linked together through Merkle trees.

Merkle trees

Merkle trees are data structures used extensively in a range of distributed ledger technologies to guarantee the integrity of the ledger and can be traced back to Ralph Merkle's thesis in 1979[17].

In the Bitcoin system the Merkle trees reside within blocks, but other distributed ledgers use Merkle trees without a block structure. As shown in figure 3, they are represented as upside-down trees with the input data (transactions) at the bottom. Each piece of input data is hashed to produce the next level up on the tree. The hashes of two pieces of input data are then hashed together to produce a new hash at the next level up. This process continues for all pieces of input data until a single hash of the whole tree is produced. This final hash at the top is called the Merkle root which provides proof of validity for all the transactions added to the tree.

Limitations of Bitcoin

System attacks

As the popularity of Bitcoin has increased, more miners operate on the system and so the processing power (also known as hashing power) increases. It is generally recognised that as hashing power increases the system is less vulnerable to attack, for example, for financial gain. However, the subversion of the process could theoretically be achieved if a considerable proportion of the hashing power is controlled. The creation of 'mining pools', where hashing power is consolidated between nodes, effectively tending towards centralisation, raises the risk of such attacks on Bitcoin being successful. It is also reported that it makes the network more vulnerable to other types of attack, particularly 'routing' attacks, so called because they attack the currency via the internet routing infrastructure[18].

Public trust

Public understanding and trust of Bitcoin is also potentially a limitation to its more widespread adoption. Bitcoin has been in existence for approximately eight years and while the DLT/blockchain community is very familiar with the cryptocurrency, and its market capitalisation is in the billions of US dollars, a large amount of the public has not heard of it or understands it, and even fewer what a cryptocurrency, blockchain or distributed ledger is. Where the public have heard of Bitcoin, it is often due to news articles that link it with nefarious activities such as payment to unlock ransomware from cyber attacks.

Scalability

At the time of writing, limitations on Bitcoin block size, in combination with the period between blocks being set to 10 minutes, restrict the rate at which transactions can be confirmed to a level that is significantly lower than financial systems, such as Visa which has a throughput of thousands of transactions per second. Discussions are ongoing in respect of the most appropriate methods to increase transaction throughput. Some key miners and developers have agreed to a 'fork' in the blockchain resulting in the original Bitcoin and a new currency called Bitcoin Cash that allows larger block sizes. Further development of the original Bitcoin is also being undertaken in order to help address its scalability challenges.

A further potential disadvantage of the limited block size is the amount of information that can be stored on the blockchain. The Bitcoin blockchain was specifically developed as a cryptocurrency and thus it was envisaged that the only data residing on the network would be that associated with transactions of currency. While it is possible to use the network in other ways, the community associated with it generally frown upon storage-heavy content being placed on it to protect against bloating of the system. In December 2016, the Bitcoin blockchain reached 100 GB and users were reporting concerns with the time taken to synchronise nodes.

Another issue facing Bitcoin, and this will be true of many permissionless systems using similar proof-of-work mechanisms, is that as more hashing power is added, the system becomes more secure but this results in more hashing power being required to mine the blocks. The system then becomes less and less usable by smaller 'players' and so due to the investment required in hardware (for example, specially designed ASICs*) and electricity, the system becomes increasingly controlled by 'groups', which then pushes it more towards more centralisation.

* See glossary page 51.

Ethereum

Like Bitcoin, Ethereum is a cryptocurrency and at the time of writing is ranked as the world's second most valuable by market capitalisation. However, Ethereum has been developed to be more than just a cryptocurrency and is described by its developers, the Ethereum Foundation, as an open platform allowing anyone to build decentralised applications on it. So, while the Ethereum platform uses a blockchain data structure and allows peer-to-peer exchange of value through its native cryptocurrency, known as ether, it incorporates a 'Turing-complete* programming language, allowing anyone to write smart contracts and decentralized applications …'[19].

The developers of Ethereum envisaged broadly three types of application of the system:

- Financial applications, that might include currencies, wills or even employment contracts.
- Non-financial, which might include voting systems or decentralised governance (for example, supply chain certification).
- Semi-financial applications which may be a combination of both. Here, smart contracts which are 'rules' written as computer code within the transaction, could allow automatic payment by a party that is in receipt of goods or service, for example, a shipment of cotton from one place in the world to another.

Comparison with Bitcoin

Some of the principles of Ethereum are similar to Bitcoin in that the ledger is still in the form of a blockchain and the system still employs a proof-of-work algorithm to secure the transactions into the blocks.

However, there are several key differences, some of which include:

- Blocks are created on Ethereum roughly every 15 seconds.
- The proof-of-work algorithm, known as Ethash, is reliant upon memory as well as CPU time. This was introduced to discourage centralisation that otherwise has been shown to result from requiring specialist processing hardware such as ASICs.

The block creation period on Ethereum facilitates a higher rate of transactions than Bitcoin, but there are still some general concerns about scalability, particularly with respect to the proof-of-work mechanism consuming large amounts of energy. The developers of Ethereum fully recognise these issues and have published a paper[20] that describes how they plan to tackle them.

One of the key differences between the two systems is Ethereum's smart contract capability. This has resulted in the system (also known as a platform) becoming popular because it provides the ability to build a range of applications on it, from games, to personal identity, to product provenance; many of these 'apps' are available at a kind of 'app store'[21]. Some of these applications are used as a means of trading things of value, such as physical goods or digital services. To facilitate this, the Ethereum platform provides the ability to create tokens or currencies that represent those items of value. As the potential capabilities of the applications have started to become realised, the creation of new tokens through initial coin offerings (ICO) has started to become increasingly popular, for example to fund the development of an application. These tokens typically raise funds by being issued to others in exchange for ether or sometimes bitcoin.

It may be seen that smart contracts have the potential to handle and trade assets of considerable value and, in such cases, it is crucial that they are secure against attacks which aim at stealing or tampering with the assets. It has been shown that some smart contracts are prone to errors that can introduce security vulnerabilities[22]. Some of these vulnerabilities have been exploited, the most successful of which, known as the 'DAO* hack', initially resulted in millions of dollars' worth of ether being drained from the DAO*.

With the ability to build many types of application on the platform, Ethereum is seen as a possible candidate for enterprise applications and, at the time of writing, the Enterprise Ethereum Alliance has recently been set up to learn about and develop enterprise solutions. The alliance is formed of large multinationals, start-ups and academics; examples of multinational launch members include Microsoft, Intel, BP, J.P. Morgan and Accenture.

* See glossary page 51.

Hyperledger

Hyperledger is a distributed ledger that uses a blockchain data structure with a very specific focus on business applications. It is described as an open source global collaboration hosted by the Linux Foundation and may be thought of 'as an operating system for marketplaces, data-sharing networks, micro-currencies, and decentralized digital communities'[23].

Hyperledger differs from Ethereum in that it is not a cryptocurrency and therefore does not have its own native currency. Nevertheless, more general finance applications are identified as potential focus applications together with healthcare and supply chain. Drawing comparison to Microsoft products, Hyperledger is being designed as a suite of products and services; the Hyperledger Blockchain Explorer for example, is being developed to create a user friendly web application to view and query blocks, transactions and associated data.

The core element of Hyperledger at the current time is Hyperledger Fabric. Hyperledger Fabric was rolled out during March 2017 and IBM, one of the main contributors to its development, announced a production ready enterprise blockchain service built on Fabric version 1.0 at about the same time.

In terms of the structure of the blockchain, Hyperledger Fabric exhibits some similarities to both Bitcoin and Ethereum; the chain provides a transaction log and is structured as a series of blocks linked through hashes of the block header. However, where Hyperledger Fabric is different from some other blockchain systems is that it is private and permissioned. Hyperledger incorporates a concept referred to as 'channels' where there is one ledger per channel and each member of the channel maintains a copy of the ledger for that channel. The members of a Hyperledger Fabric network are managed by a membership services provider and a Hyperledger network therefore does not need to employ an energy intensive proof-of-work algorithm to achieve consensus.

An early example of the use of Hyperledger is Everledger and its first application was providing transparency over the provenance and tracking of diamonds.

Corda

Corda is a distributed ledger platform developed by a consortium known as R3 which comprises some 80 of the world's financial institutions and regulators. Corda has been designed specifically for financial services purposes and, with banks generally being early adopters of new technologies, it is a relatively mature platform.

The introductory whitepaper[24] describing Corda refers to a number of key principles that drove its design. Key to this was a desire for the facts recorded on the ledger to be accepted as admissible evidence in the case of a dispute. Furthermore, the facts recorded should be irreversible to the extent that where errors occur they would have to be corrected through additional transactions to ensure full transparency of what has happened, so incentivising organisations to tighten quality management processes. Of particular importance were privacy and the need to ensure that any records on the system should only be accessible to those for who access is necessary.

Corda was designed as a ledger with a peer-to-peer architecture within semi-private networks. Admission requires obtaining a network identity from an authorised party and cryptographic signatures are used to identify parties and data.

A key characteristic of Corda is that there is no blockchain; each node of the network maintains a database of shared facts, namely those it has shared with other nodes, and these shared facts are called 'states'. States are immutable and the facts that they contain typically include information such as stocks, identity data and contract conditions. The transactions within Corda represent proposals to update states on the ledger and for a transaction to be valid they must be signed by the appropriate validators. Consensus on the network is achieved using one or more 'notaries'* who ensure that double spending does not occur. Corda allows notaries to choose the consensus algorithm based on the requirements for privacy, but the system does not use miners or proof of work.

The particular architecture that forms Corda means that nodes only process transactions if they are involved in them in some way. As a consequence, Corda does not suffer the same concerns with scalability that are present with some other distributed ledger systems such as Bitcoin.

* See glossary page 51.

Types of distributed ledger technologies compared

	Bitcoin	Ethereum	Hyperledger	Corda
Cryptocurrency required	Bitcoin	Ether, user-created cryptocurrencies	None	None
Network	Public	Public or permissioned	Permissioned	Permissioned
Transactions	Anonymous	Anonymous or private	Public or confidential	Confidential
Consensus	Proof of work	Proof of work	Practical Byzantine fault tolerance*	Supports a variety
Smart contracts (business logic)	None	Yes (Solidity, Serpent, LLL)	Yes (chaincode)	Yes
Language	C++	Golang, C++, Python	Golang, Java	Various compatible with Java virtual machines

Table 2: Comparison between Bitcoin, Ethereum, Hyperledger and Corda (Sources[24, 25])

Application of distributed ledgers in engineering

The systems described in the previous section are high-profile examples that demonstrate many of the core underlying principles that form DLT/blockchains. Ultimately, some engineering challenges might be addressed by utilising some of these more off-the-shelf solutions, while others will demand them to be more tailored. A key issue that must therefore be addressed is how to determine whether these technologies can address a particular challenge and, if so, how to go about selecting a solution.

A key issue that must be addressed is how to determine whether these technologies can address a particular challenge and, if so, how to go about selecting a solution.

In undertaking the research for this report, a number of perceived opportunities for DLT/blockchain within engineered systems were identified. Table 3 overleaf summarises the findings which build upon ideas considered in the UK government review of distributed ledgers and support themes identified in the Foundation's foresight reviews, particularly those of big data[26] and resilience engineering[27].

The need for auditability and transparency of data and information applies across the industry sector categories is considered in this section. Verifying product provenance, qualifications and experience of personnel or system operation, are all key aspects in providing assurance of performance, dependability and safety of engineering systems.

Security and privacy of data and networks, are also key themes that emerge, particularly in the context of IoT (internet of things) and smart networks. Security and privacy are increasingly important as assets become more interconnected, with DLT/blockchain potentially forming part of the solution to achieving robust smart manufacturing or smart energy metering systems.

In order to help assess whether DLT/blockchain is appropriate in a given situation, as compared to some other solution, it is useful to consider a number of questions[28]:

- Do you need a database?
- Does it require shared write access by multiple parties?
- Is there any mistrust of those writing parties?
- Would an intermediary resolve the issue of trust?
- Is there a need or desire for functionality to be controlled?
- Is there a desire for transactions to be public?

The actual solution will very much depend upon the specific scenario, but it may be seen that a key element in this is whether there is any mistrust of the writers to the system.

There are already many examples of where application of DLT/blockchain is being investigated as a solution to certain engineering challenges. While such examples are at varying stages of development, from early research in academia to advanced pilot studies by technology start-ups and multinational corporations, the levels of investment being committed suggest that such systems do present valid solutions for certain applications. In order to demonstrate this, a number of examples are discussed in more detail in this section.

Table 3: Opportunities for DLT/blockchain in addressing engineering challenges

Engineering challenge \ Sectors	Transport and critical infrastructure	Food
Information theft	Prevent theft of building space and time usage information Track information on products subject to export control	
Disruption or prevention of operation	Secure vehicle communications and logging	Cold chain monitoring, positive testing alerts or post recall crisis root cause analysis
Corruption and falsification of sensor data		
Falsification of information	Verification and transparency of technical staff qualifications Smart identity and payment on transport services Air traffic verification eg drones	Ensure validity through transparency of labelling and sell-by dates Ensure food provenance
Information silos	Secure sharing information between rail networks, system components and management systems	Secured and efficient information flow (eg from farm to fork)
Additional potential applications for societal benefit		
Tracking of endangered species Tracking of distribution of international aid		

Healthcare and medical	Energy	Manufacturing	All these sectors
Secure log of usage of patient data health records	Consumer smart metering protection	Secure log of usage, maintenance, quality control statistics	Prevent intellectual property theft
		Facilitating just-in-time delivery through securing interconnected systems	Hacking of software Accidental changes in software – provide authentication and logging Prevent denial of service attacks in networks (Including Internet of Things [IoT] devices)
		Secure log of use of health and safety equipment	Transparent log of sensor data
Identity and verification of care providers Preventing counterfeit pharmaceuticals and cosmetics	Provide assurance of ethical power Immutable and transparent tracking of industry waste eg nuclear		Traceability and transparency for auditing in supply chains to combat counterfeiting Assurance of designs, (3D models, FE, CFD)
Secure sharing of information between doctors, hospitals, health authorities	Provide smart connection between automakers, consumers, energy companies (eg about battery lifecycles)		

Physical assets and people

One of the main areas of potential application of DLT/blockchain within engineering, that is both evident in table 3 and supported by a number of real-world examples, is in providing assurance of the provenance of people or assets.

An early example of such an application is that of Everledger, which is using distributed ledger technologies to track diamonds, providing transparency of their provenance by utilising the unique characteristics of the diamonds and registering these on a blockchain. It has also been reported that it is looking into expanding the system's use to track the provenance of wine and fine art[29, 30].

An example of a similar organisation which has attracted the attention of major brands is Project Provenance Ltd. Its mission is to 'help businesses share open, honest data about products, so that end customers can make informed purchases'[31], and while its focus so far has mainly been on the food sector, examples of other consumer goods are cited on its website. Project Provenance is explored in more detail in the case study on page 35.

Having an understanding of the provenance of products is extremely important, particularly in areas such as pharmaceuticals and engineering supplies, where the risks of counterfeit products could have profound consequences on safety or the environment during manufacture, in use, or disposal. While industry sectors have existing processes for doing this, true global and through-life transparency rarely exists. This transparency would enable counterfeit products or exploitation of people to be quickly identified and incentivise the supply of genuine goods within the supply chain. Furthermore, with systems such as Ethereum providing smart contract capability, ownership or certification status of assets could be recorded on the ledger; subsequently, when a product or service is transferred to another party, the record of this transaction would be recorded on the blockchain and automatic payment could be coded within the transaction.

On a broader scale, the technology could have the potential to assist in addressing sustainable development goals set out by the United Nations. One of the goals where investment in applications of distributed ledgers is being made is that of goal 16.9, 'by 2030, provide legal identity for all, including birth registration'[32]. An organisation called AidTech is utilising the technology to facilitate digital identities and provide transparency in the delivery of humanitarian aid[33]. Organisations such as Deloitte are also investing in distributed ledger technology solutions to address the global identity problem[34].

However, many of these potential applications remain theoretical with challenges, such as how to reconcile DLT/blockchain transparency with the privacy requirements of an identity register and who should control the data, still needing to be tackled. Furthermore, while

solutions to challenges such as providing links between physical products and their digital ledger representation have been demonstrated, the application of such solutions to the scale and complexity of, for example, the automotive industry supply chain needs to be validated.

A centralised data management system exists in the automotive industry known as the International Material Data System (IMDS). Hosted by DXC Technology (previously Hewlett Packard Enterprise), it provides a single portal where 'all materials present in finished automobile manufacturing are collected, maintained, analysed and archived'. Thirty-three name-brand manufacturers, representing 56 different brands of vehicles, and more than 120,000 (Tier 1 and lower) automotive suppliers of materials and components use the system. It is stated that with evolving legal requirements related to environmental issues, increasingly countries require automotive manufacturers to track the substances in the finished product and report on them to various legal entities. IMDS allows this exchange of information[35].

Data as an asset

As highlighted previously, one of the key themes emerging from the research for this report was that of ensuring security and privacy of data and information, while having assurance over its provenance.

Digital systems are commonplace in modern engineering environments and for critical infrastructure, such as railway networks, they are likely to be adopted even more widely in order to further improve performance[36]. Certain elements of functionality of these systems can be critical to the safety, dependability or environmental impact of an asset and, in recent years, communications technology has been further transforming the way industries work. IoT devices are becoming ever more pervasive with Gartner estimating that 8.4 billion connected 'things' will be in use in 2017, and will reach 20.4 billion by 2020. It is also estimated that business IoT spending will represent 57% of overall IoT spending in 2017[37].

Distributed ledger technologies potentially hold key benefits in the management of such systems[38]. Their distributed architecture is particularly suited to a network of distributed devices; peer-to-peer communication not only potentially reduces the cost associated with deploying centralised control systems, but it provides a means of preventing single point failure. Cryptographic mechanisms ensure that communication between devices is secure and that logs of data flows are maintained as permanent records. Transparency ensures that the details of data flows, such as who or what has accessed the data, are visible, incentivise greater rigour in design and quality control and also potentially speed up the process of learning from malfunctions and accidents. The provision of smart contracts on platforms such as Ethereum potentially offers an additional dimension to the capability of such systems, allowing such networks to function in autonomous ways. Examples of applications being investigated by both academia and energy companies include smart energy management, offering the ability to manage intermittent loads (for example, from solar or wind sources) on a power grid while providing the financial mechanisms to enable this[39].

An application that transcends both the physical and digital environments is maintenance, and this is an activity that is crucial to safety of assets. Such a possible application was highlighted in a talk, Blockchain for beginners,[40] given by Andreas M Antonopoulos where he indicated that he had discussed using the technology to provide an immutable record of maintenance activities and parts used. In some industries, maintenance activities are heavily regulated and an asset such as an aircraft might have maintenance carried out regularly in different parts of the world. Having instant access to a global, immutable log of who carried out such activities and what they did would be highly beneficial for operators and maintainers, equipment providers, and regulatory bodies. Similarly for automotive, it could provide clear visibility, both to the car manufacturer and to the vehicle owner as to exactly which activities have been carried out. In some industries, such as shipping, the technology has the potential to radically transform the whole practice of maintenance.

There are many applications in engineering where initially it might be viewed that distributed ledgers or blockchains provide an ideal solution to a particular challenge, but careful consideration needs to be given to the problem in order to understand whether this is the case. Examples of systems exist, such as for providing a secure log of usage of patient health records, that use some of the underlying technologies of blockchain, but do not actually employ blockchain architecture because it would have introduced unnecessary complexity and inefficiencies in use of the system.

Case study 1: Asset safety – Marine Transport International

An example of where distributed ledger technology is being deployed directly to enhance safety is in the verification of mass of shipping containers. Since 1 July 2016, the International Maritime Organization's SOLAS Convention has required shippers to verify the gross mass of packed containers before they are loaded on-board the ship. Marine Transport International UK Ltd (MTI), an organisation that focuses on digital supply chain engineering has leveraged the MAS Protocol by Agility Sciences Ltd in its ContainerStreams product to deploy commercially scalable distributed ledger technology in the container shipping industry in order to provide this capability.

The MAS Protocol is a multi-threaded ledger, which stores and transmits data in a multitude of simultaneous chains of activity, an innovation labelled activity streaming. It is reported that the technology developed provides an answer to addressing the performance and scalability challenges associated with other systems. Furthermore, the MAS protocol was designed to be interoperable with existing infrastructure, including legacy IT systems, with the goal of creating ease of implementation and usability.

ContainerStreams provides a means to connect landside parties, load point, weighbridge, trucker, shipper, carrier and terminal, and allows the verified gross mass of the container to be to be transmitted to the carrier terminal before the container arrives. Once a container has been loaded with its cargo, it is weighed and the details are subsequently uploaded to ContainerStreams via an application. The carrier and terminal are then able to verify the details uploaded to the system. The technology therefore allows for increased health and safety within ports and for preventing overweight containers from being moved across transport networks. The software application has also created increased supply chain visibility and transparency for customers who are using this technology.

Case study 2: Supply chain transparency – Project Provenance Ltd

Project Provenance was started from a frustration of how little society knows about the products we buy. Driven by environmental concerns, conscious consumption is a globally growing behaviour and Provenance believes that blockchain technology provides a way for people to know with certainty a product's origin, its characteristics and ownership, empowering people to change the way products are bought.

Provenance utilises an open blockchain platform to provide traceability and transparency of everyday consumer products. A recent case study detailed on Provenance's website[41] highlights the benefits through the development of a system that enables the tracking of tuna, from catching them in Indonesia to point of sale.

The process was initiated with an analysis of the point of origin. It was recognised that specific infrastructure and equipment for identification of the fish was limited but most of the fisherman, suppliers and factory workers had mobile phones.

Provenance developed a system that utilises a simple smartphone interface, linking identity, location, material attributes, certifications and audit information with an item or batch. Fishermen sent SMS messages to register the catch, thereby adding a new asset to the blockchain. Accompanied by unique identification, the fish were transferred from the fisherman to the supplier along with their representation on the blockchain. Social and environmental conditions for the fisherman are verified by trusted third parties who validate compliance against defined standards.

The project then went on to investigate and develop solutions for integration with existing business systems. Challenges included consideration of what happens to the product when it is packaged, how to represent this on the blockchain, and how the packaged product should be identified and marked. The solution included the provision of QR code labels to allow scanning through the next stages of the supply chain.

The final stage of the pilot involved developing a suitable solution for the customer experience which resulted in the replacement of traditional printed communication with online product stories available through mobile devices and activated through near field communication* enabled smart stickers on the product.

* See glossary page 51.

The work conducted by Provenance has demonstrated that the values of trust, transparency and ethical sourcing are extremely important in modern society, and that blockchain technology has the potential to radically change the status quo in assuring products. 'Openness, honesty and social responsibility' (Co-op/Provenance, 2017) are part of the ethical values of UK supermarket, Co-op, and the two organisations are now working together to explore how blockchain technology might help to support these.

DLT/blockchain technology challenges

In making an assessment of any solution that might address an engineering challenge, it is necessary to understand both its capabilities and its limitations. Especially in considering that DLT/blockchain are relatively immature technologies, the challenges associated with their application must be clearly understood and further detail of these is explored within this section of the report. It may be seen that generally, the challenges of the technology are horizontal, which is to say that the same challenge applies across industry sectors.

In making an assessment of any solution that might address an engineering challenge, it is necessary to understand both its capabilities and its limitations.

Interfaces and interoperability

The interface with physical goods

The Provenance project detailed on the previous page highlights where a team developing a blockchain-based system have thought about the system integration issues that need to be considered and demonstrates real world application in providing assurance of engineered systems. For many applications being discussed, the distributed ledger is just one element of a complex system that helps to provide a solution to certain challenges. While it could be argued that many of the issues referred to in this section are not specifically associated with distributed ledgers or blockchain, there are nevertheless unique challenges associated with their interfaces that require careful consideration.

If distributed ledgers are to be used in supply chain applications, they will have to interface with product identification solutions. The Provenance system developed for tracking tuna uses an address on the blockchain to provide the unique identity of the product and this is then linked to the physical product through a 2D barcode* or near field communication device.

Solutions will also need to be developed that take account of existing means of product identification. Standards such as the Electronic Product Code (EPC) developed by GS1 are increasingly

* See glossary page 51.

being adopted in sectors including retail, healthcare and transport. These standards cover not only the characteristics of the identifier, but how this should be represented in whatever method is used to mark the product, whether it be for example a 2D barcode or an RFID (radio frequency identification) tag.

The security of a system is only as good as its weakest point, and while the cryptographic techniques used in the digital domain might present a mathematical improbability of subverting the system, existing methods of physically marking products are themselves vulnerable to counterfeiting or alteration. One way of tackling the problem is to ensure that the means of product identification (marking is one method) is as unique as the cryptographic hash to which it refers. In recognising that any change to the input of the hashing algorithm will produce a unique output, existing methods of product identification such as stamping might be used or adapted and linked through a photograph. More secure approaches might involve other forensic techniques that recognise the inherent uniqueness of the product such as grain structure in a metallic material or material isotopes. The solutions to prevent counterfeiting of bank notes and coins might also be considered.

The interface with business systems

Even before the advent of the internet, businesses have been looking at ways in which digitalisation can streamline and improve the effectiveness of their processes. Manufacturing in particular, in many parts of the world, has embraced digital tools and through their implementation continues to achieve higher quality and greater output. While there is room for improvement in the way that these systems are integrated, many businesses have implemented systems such as SAP or Oracle which may incorporate enterprise resource planning (ERP) tools. Engineering organisations are also increasingly turning to product lifecycle management systems such as those offered by Siemens or Dassault Systèmes, and it has already been shown in this report that they might use global systems, such as IMDS, in the automotive industry (see page 32).

The investment required to implement such systems is typically high and it will be embedded usually within company processes. Consequently, while some businesses may be prepared to adopt new technologies, a key aim for development of DLT/blockchain should be to make them business system agnostic. In this respect, organisations such as SAP are investing in blockchain, demonstrated by an announcement in May 2017[42] of its integration with its Leonardo platform. With a strong focus on enterprise systems, Microsoft too recently announced its Coco Framework, a system that aims to deliver enterprise-ready solutions in which existing blockchain protocols such as Ethereum, Hyperledger Sawtooth and Corda can be integrated. A key consideration by consortia such as the Enterprise Ethereum Alliance will be the integration and interfacing of such technologies with existing systems.

Human interfaces
The human interface is arguably one of the most important interfaces to consider as ultimately, humans will have to communicate with the system somewhere, whether it be in design, implementation or in-service.

If distributed ledgers are to gain more widespread adoption, good understanding of the philosophies that underlie the platforms, and the associated software code through which they are developed, is essential. This is not only for the developers using or trying to interface with them, but for providing assurance to customers, regulatory bodies and third party certification bodies that they meet the relevant requirements. Most of the main platform developers are publishing detailed whitepapers that describe what is needed to interact with the system. Furthermore, the underlying code of many of the platforms is open source and the programming languages that might be used to develop applications are widely understood.

Organisations such as Microsoft are also assisting in this respect. As a launch member of the Enterprise Ethereum Alliance it will be looking to understand the needs of enterprise users and the impacts this will have on delivering blockchain as a service. This work has already

been started under its Project Bletchley initiative where it has been developing support for blockchain on its Azure cloud computing service. At the time of writing, Microsoft had recently released an Ethereum Consortium Blockchain Network solution template within Azure Marketplace (like an app store) allowing the deployment and configuration of a private Ethereum network from the Azure portal with a single click. The user interface that allows the system to be set up is similar to other Microsoft products and is relatively intuitive to use. Such aspects, especially in respect of being able to interrogate or visualise the information contained within the system, will be also be important in allowing for greater adoption of the technology. Such importance is underlined by the fact that IBM have also been investing heavily in blockchain technologies and indicate on its website that with its blockchain service on Bluemix*, 'you can also create and deploy a private blockchain network (a clone of the Hyperledger Fabric) in one click'.

Building public understanding and trust

Public understanding and trust in DLT/blockchain is crucial to enabling it to fulfil its potential. The first critical step in this process is to provide a universal understanding of the terms. At the present time, if the term 'blockchain' is used, one party might understand it to mean a completely decentralised and distributed ledger, while another might be referring to it in the broader family of technologies' sense.

Once this foundational baseline has been set, it is then easier for conversations to take place around the benefits and the limitations of the different technology options in the context of the specific industry challenges faced. Engineers across a variety of disciplines would benefit from a broad understanding of the capabilities of the technologies and specifically how to assess whether they might be suitable for particular applications. Education about the technology through channels such as training courses and documents, including this report, supported by discussions led by well-respected public figures, will help to further this understanding. Where a clearer scope is defined in respect of a particular need, workshops exploring specific domain challenges and identifying potential solutions for pilot studies would be beneficial.

Ultimately, the level of understanding required will be highly dependent upon an individual or organisation; Steve Jobs[43] is reported to have said that technology should either be invisible or beautiful and it is arguable that DLT/blockchain are currently neither of these things.

* See glossary page 51.

Scalability

Scalability is one of the challenges of blockchain that is written about regularly within the community and has previously been mentioned in the section discussing Bitcoin and Ethereum. Scalability is an inherent issue associated with open, permissionless systems, where the perceived security of a centralised system is typically exchanged for a currency-based reward system (for example, proof of work).

This issue is a concern because if businesses are going to invest in blockchain (permissionless) systems to underpin critical business activities, in addition to needing to know that the system is secure, they need to be assured that: the processing power required to maintain this security is not going to become economically unviable and environmentally unsound; that the database is not going become infeasibly large; and that transaction throughput will be sufficient for their needs.

In light of the scale of concern around this issue, there is a significant amount of work being undertaken to address it. One route to addressing the problem is to use permissioned systems, such as Hyperledger, where computationally-heavy consensus algorithms are not required. Such solutions however raise questions as to the added value when compared to typical distributed databases. Hybrid solutions such as RSCoin[44] have also been proposed where some level of centralisation is reintroduced while maintaining transparency and increasing transaction throughput. One of the stated aims of the Enterprise Ethereum Alliance is to address performance issues and recently, Vitalik Buterin a co-creator of Ethereum has published a 'mauve paper'[20] which sets out proposals for how scalability on the Ethereum system will be addressed. It involves changing the consensus mechanism to a concept known as proof of stake*, together with a mechanism commonly used in distributed databases known as sharding*.

As it might be imagined, there are also some prominent national and international organisations investigating how such issues might be resolved. Intel have been undertaking work on a project known as Sawtooth Lake[45] described as a modular platform for building, deploying and running distributed ledgers. In place of proof of work, the Sawtooth Lake platform includes a consensus mechanism that uses proof of elapsed time with what is termed a 'trusted execution environment' such as Intel Software Guard Extensions (SGX)[46] to ensure safety and randomness in electing the node that creates the block. The aim of this approach is to provide a more economical and greener algorithm.

* See glossary page 51.

The UK's National Physical Laboratory (NPL) has also been conducting work focused on increasing throughput of transactions and is about to conduct an experiment in which Coordinated Universal Time (UTC) timestamped stock trades generated from atomic clocks are compared to locally-created, untraceable timestamps and recorded on a distributed ledger. The project, known as the Atomic Ledger, will record over 20 million transactions over a few hours of trading. NPL believes that the application of precise, traceable and certified timestamps, as applied to the nodes of a distributed ledger system, could enable a trusted approach to determining the existence of transactions at that point in time, across all platforms.

Privacy

Privacy is a controversial subject in the context of distributed ledgers and alongside scalability is one of the most discussed. One of the key benefits for many of the applications of distributed ledgers is the ability to provide transparency over the transactions recorded in the ledger. But while there are stakeholders that will find such a characteristic of benefit the level of transparency desired varies from one to the next and very few want every piece of information being visible to a public database.

The research highlighted potential concerns associated with applications where real-time data might be being used, such as in autonomous vehicles, or revealing passenger information where such a system might be used for payments in travel. A similar concern around potential uses for smart metering was also raised where private data about usage of energy could reveal space-time information about the building usage.

As with the challenge of scalability, one of the seemingly obvious solutions is to use a permissioned ledger. Such a system could be arranged so that different levels of permission are given, while allowing access to any party that needs to audit the system. The benefits and drawback of using such a system have already been discussed within the distributed ledger technologies in detail section of this report (page 15).

For permissionless systems, one of the key challenges is how to transact privately in a completely open system, while at the same time revealing to whoever you wish the exact transactions you are undertaking. A solution that has been developed is known as Zcash[47] which allows payments on a public blockchain while the sender, recipient and amount can remain private. The system relies on a concept known as zero-knowledge proof systems, introduced by Goldwasser, Micali and Rackoff[48].

There are a number of proposed solutions to address the issue of privacy and these have been discussed at some length in a blog post by Vitalik Buterin, Privacy on the Blockchain, where he states that specific solutions will depend on a certain application[49].

From a technical and ethical perspective, privacy is still an area that requires some consideration and benefit would be gained from undertaking a study in considering specific privacy solutions against types of DLT/blockchain system in particular applications.

Governance

Structure and organisation

One description typically given to distributed ledger technology platforms such as Bitcoin is that they are decentralised. If they are considered purely in the context of their physical architecture, then this description can, for many of them, be true. However, the term decentralised also refers to the way in which they are governed and while a view might be that platforms such as Bitcoin have decentralised governance, there is an increasing view that this may not be the case.

Vili Lehdonvirta, an Associate Professor at the Oxford Internet Institute of the University of Oxford and a contributor to this report, explains[50] that in an economic organisation, there must be a distinction made between enforcing the rules and making the rules. The Bitcoin Protocol is a set of rules that are enforced by the network, but one must also consider who defined these rules. The initial protocol was written by Satoshi Nakamoto, with later versions being released by the core development team, a relatively small group of individuals. Furthermore, with a large percentage of the hashing power on the network being in the hands of a relatively small number of groups, many of whom are located in the same area of the world, they potentially have the ability to influence the direction that the network might take.

Recent news has only served to further highlight this issue. With a long running debate that focuses on the size of Bitcoin blocks and with little formal governance process in place, different factions were in disagreement and the blockchain was 'forked' with different branches running different versions of the code and the potential for the value of assets on one of them to become worthless. Lehdonvirta proposes therefore that blockchain technologies cannot escape the issue of governance and that, once this has been recognised, it raises the question as to what value a blockchain provides over more conventional technology.

Organisational and governance issues are therefore a key element of DLT/blockchain that will need to be considered and the approach taken, as has been seen in examples presented, will ultimately depend on the specific situation. Solutions to the broader challenges of structure and organisation may lie in the formation of consortia, such as those of R3, Ethereum or Hyperledger, or public-private partnerships might also be a potential model.

Regulatory environment

A further aspect that is only recently starting to be considered in any depth is the regulatory environment that might impact on the use of DLT/blockchain.

At the time of writing, the regulatory landscape for cryptocurrency-based distributed ledgers such as Bitcoin is changing regularly, with some countries considering specific regulation while others are taking a wait-and-see approach. Generally however, there is little specific legislation written around the broader use of DLT/blockchain technologies.

Governments and research teams are starting to investigate the potential questions that relate to their use such as:

- What is the legal status of smart contracts?
- What are the liabilities of developers if something goes wrong, for example, what if a flaw in the code or system is a contributor to a safety hazard.
- With such systems crossing international boundaries, which country would have jurisdiction, for example, if someone loses money in using them.

One group starting to consider such questions is the Microsoft Cloud Computing Research Centre. Launched in April 2014, it is a collaboration between the Cloud Legal Project at the Centre for Commercial Law Studies, Queen Mary University of London and the University of Cambridge Computer Laboratory and is looking to address a wide range of legal issues in cloud computing, including distributed systems, networking and security.

Standardisation

There are currently few standards that specifically relate to DLT/blockchain technologies and it might be argued that standardisation could be both an opportunity and a challenge for their ongoing adoption. In many ways, the debate over standardisation leads on from that of governance. Earlier in this report, distributed ledgers and blockchain were defined in terms of a number of characteristics and there will be areas of the community that feel that standardisation not only invokes a level of centralisation but, if implemented in the wrong manner, could stifle innovation.

Nevertheless, standardisation typically also has a benefit of allowing more widespread adoption. For many of the applications discussed throughout this report, standardisation is an integral part of governance systems and the engineering community will expect some level of standardisation, not only to allow interfacing and interoperability with other systems, but to provide protection against obsolescence in light of investments being made and to help maintain the security and privacy of the technology. In this respect, ISO has started to consider these technologies under ISO/TC 307, Blockchain and electronic distributed ledger technologies. The scope of the group is 'standardisation of blockchain technologies and distributed ledger technologies'. The British Standards Institution has formed a committee, DLT/1, on blockchain and electronic distributed ledger technologies to pass the UK view to ISO and develop other standards, and it has recently published a report with RAND Europe detailing the challenges, opportunities and the prospects for standards[8].

Assurance of provenance within supply chains is identified as a potential application for distributed ledgers and this is an area in which there is already a degree of standardisation. In this respect, an example of an existing standard that has seen increasing adoption across

various industry sectors is that for defining GS1's EPC together with its Electronic Product Code Information Services (EPCIS). The purpose of EPCIS is stated as being to enable trading partners to share information about the physical movement and status of products as they travel throughout the supply chain and is published as an ISO/IEC standard. GS1 have recognised the importance of distributed ledger technologies in such applications; a news article published in January 2017[51] indicates that GS1 are working with Microsoft on blockchain product tracking under the project name, Project Manifest.

Quantum computing

Many of the challenges so far considered in this report are known issues for which solutions need to be investigated to make DLT/blockchain viable for a range of applications being considered. However, a potential risk for these technologies that will also need consideration is the effect of quantum computing.

Quantum computing is still in its early infancy and therefore is not likely to pose an immediate problem. However, it is reported that a quantum computer could threaten the security of signature schemes such as those used in Bitcoin and as a result it is important to consider the security of DLT/blockchain in a 'post-quantum' setting; an article on Bitcoin.com in December 2016[52] highlighted that: "The National Security Agency (NSA) recently issued a warning about the threat of a quantum computer. 'A sufficiently large quantum computer, if built, would be capable of undermining all widely-deployed public key algorithms used for key establishment and digital signatures'." There are already signs of research that are looking at the potential threat and Ericsson have published an article[53] detailing the reasons why existing hash functions such as SHA-256 already offer strong resistance to a quantum computing threat.

Findings and recommendations

The emergence of Bitcoin and associated distributed ledgers has led to a dramatic increase in innovation in DLT/blockchain technologies. It might be argued this is innovation in the truest sense; just as with Bitcoin, it is often application led and challenges that have faced industries for decades such as counterfeiting now have technological solutions to help combat them. Furthermore, with an increasingly data-centric society, the people and organisations that generate this data and for whom it holds tremendous value, now have a way of controlling its use.

The primary question that this study sought to answer was whether engineering can use distributed ledger and blockchain technologies to the benefit of assurance and safety.

The primary question that this study sought to answer was whether engineering can use DLT/blockchain technologies to the benefit of assurance and safety. As should be the basis of any engineering challenge, it is important to fully understand the requirements rather than presupposing the solution. While a distributed ledger, or a blockchain, might be ideal for specific scenarios, there may be more mature technologies that can provide the capability desired. There are systems in development that could quickly address the current compromises of blockchain such as scalability. With the relatively low throughput of transactions, many blockchain based solutions would currently be unsuitable where real time analytics of truly big data is required.

The level of activity associated with applications of DLT/blockchain technologies in engineering is rapidly increasing. Early work conducted by entrepreneurial technology companies has demonstrated real applications, investigating and tackling some of the key challenges associated with the technology itself. Large multinationals across engineering intensive industry sectors, such as aerospace, shipping and energy supply, are also investing to determine the potential benefits.

Assurance and certification

Distributed ledger technologies could have a major impact in areas such as supply chain assurance, maintenance and product certification. Heightened environmental awareness within society due to major climatic events and socio-economic issues, such as national protectionism, mean that transparency over the provenance of products and the qualifications and experience of people is becoming ever more important in demonstrating that customer, safety and sustainability standards have been met.

While the adaptable nature of the underlying technologies means that they have the potential to provide benefits in this space, the specific benefits of DLT/blockchain are still to be widely proven. In this respect a number of key aspects remain to be more fully addressed:

- Interfaces with the physical world
- Integration with existing business systems
- Structural and organisational considerations.

It is considered that further research is needed in these areas, with both academia and businesses having key roles to play. Benefits would be gained from more focused leadership within well-established industries such as food, automotive, aerospace or pharmaceuticals where the impacts could be the greatest, for example in preventing counterfeiting to improve safety. The Lloyd's Register Foundation is in an appropriate position to take a key role in developing, for example, consortia to help drive understanding and development of common approaches across the sectors.

Additionally, further investigation needs to be conducted into developing understanding of the legal implications of using such technologies, particularly across international boundaries. Furthermore, with currently little formal governance in place, providing assurance over the integrity of the technology platforms themselves needs to be addressed.

Public trust and understanding

With the rapidly increasing role of data in our everyday lives, for example in health monitoring, individuals and businesses need to be assured of provenance and quality of data, and that they are obtaining value for the information developed from it. Distributed ledgers have the potential to help provide this assurance through delivering an immutable log of what happens to that data.

However, people need assurance that the systems put in place to provide that transparency can be trusted to do so. It is interesting to note that even after approximately eight years of being in existence, many people have not heard of Bitcoin, and even more have not heard of distributed ledger or blockchain technologies. It should also be noted that many engineers and technical experts have not heard of these technologies and it is this community that might be expected to be involved in its implementation. Often when the technologies are mentioned in news items it is associated with descriptions of illicit trade which serves to raise doubts about its use. If the technology is to provide the benefits for which it has potential, there needs to be a greater understanding of it.

The level of training available in the subject is limited and with a large amount of documentation on the internet from a wide range of sources, it can be difficult without significant research to know which to trust. It is proposed that the Lloyd's Register Foundation and The Alan Turing Institute are in a good position to help develop training alongside trusted professional bodies. Due to the complexity of the subject matter, it would be beneficial to have a range of levels of training suited to the trainee's prior experience and the context in which they are going to use the skills developed.

It is also suggested that the development of standards by recognised bodies helps to build trust in technologies. Lloyd's Register Foundation is linked to a range of industry sectors that might be impacted by the technology and it is suggested that closer ties with the technical committees developing standards would be highly beneficial.

Technology road mapping and development

The report identifies a range of technologies and number of distributed ledgers and databases underpinned by them, but only to the extent that is necessary to demonstrate the variation in characteristics and potential capabilities that could be achieved. There are a number of underlying technologies that this report does not cover in depth, as well as a wide range of distributed ledger and distributed database platforms that could potentially be used to deliver against the industry challenges identified.

A major challenge for the industries, particularly in light of the general lack of knowledge or understanding, and the level of maturity of the technology, is in selecting a solution that meets the specific needs of that industry or specific stakeholder.

There have been a number of attempts to develop models to assist in deciding what kind of solution is needed and that developed by Bart Suichies[54] on the basis of an article written by Gideon Greenspan[28] is considered a good framework on which to start.

In light of the increasing range of solutions available, and the lack of clarity over their level of maturity, it is considered that the Lloyd's Register Foundation and The Alan Turing Institute should develop a detailed mapping of:

- Technologies already identified as underpinning DLT/blockchain and distributed database systems.
- The range of technology solutions in existence that might be used for the applications in this report (which might include solutions other than distributed ledgers or blockchain).
- The related technologies (for example, detailed in papers) that might be used to further enhance, or present a threat to the characteristics (for example, security) of DLT/blockchain.

The map should detail the technology readiness level (TRL) of each underpinning technology and platform solution and should plot each of them against the engineering applications, citing benefits and drawbacks (for example, interoperability with business systems). This would allow industries, systems designers and integrators to be better informed about which type of system is best suited to their specific needs.

Finally, the Lloyd's Register Foundation should maintain a watch on funded programmes of research from bodies such as the EPSRC. Additional sources of information and examples of areas of research being undertaken are provided in the appendix.

Appendix: Glossary, references and further reading

Glossary of terms

Application-Specific Integrated Circuits (ASIC)	An ASIC is an integrated circuit (IC) that is customised for a particular purpose. One of these purposes is mining for cryptocurrencies.
Bluemix	IBM's cloud platform, its equivalent of Microsoft's Azure.
Decentralised autonomous organisation (DAO)	A DAO is one type of application of smart contracts.
The DAO	The DAO refers to a specific DAO conceived by the team behind Slock.it which is described as a universal sharing network.
Near-field communication (NFC)	A set of communication protocols that enable two electronic devices, one of which is usually a portable device such as a smartphone, to establish communication by bringing them within 4 cm of each other
Notary	A network service that provides uniqueness consensus by attesting that, for a given transaction, it has not already signed other transactions that consumes any of the proposed transaction's input states. https://docs.corda.net/key-concepts-notaries.html
Practical Byzantine fault tolerance (PBFT)	A type of algorithm used in distributed systems to achieve consensus on the contents of a database between nodes within that system.
Proof of stake	A type of consensus algorithm that requires the prover, that is the node attempting to create a block, to show ownership of a certain amount of 'money'.
Sharding	An approach to distributing 'chunks' of data within a database to improve the throughput and overall performance where high-transaction rates are anticipated.

Sybil attack	A type of attack in computer security where a reputation system is subverted by forging identities in peer-to-peer networks.
Turing-complete programming language	A language that lets you specify any functionality that is possible to be specified by any other computer.
Two-dimensional (2D) barcodes	Squares or rectangles that contain many small dots; these can hold a significant amount of information and may remain legible even when printed at a small size or etched onto a product.

References

Note all url's accessed 9 September 2017.

1 Government Chief Scientific Adviser (2015). **Forensic science and beyond: Authenticity, provenance and assurance.** Annual Report. The Government Office for Science, London www.gov.uk/government/publications/forensic-science-and-beyond

2 Government Chief Scientific Adviser (2016). **Distributed ledger technology: beyond block chain.** Blackett Review. The Government Office for Science, London www.gov.uk/government/publications/distributed-ledger-technology-blackett-review

3 Nakamoto, S. (2008). **Bitcoin: A peer-to-peer electronic cash system.** https://bitcoin.org/bitcoin.pdf

4 **Why engineering matters.** (no date [nd]). https://engineeringthefuture.co.uk/why-engineering-matters/

5 Royal Academy of Engineering and The Institution of Engineering and Technology (2015). **Connecting data, driving productivity and innovation.** RAEng, London. http://www.theiet.org/sectors/information-communications/topics/connected-data/articles/connected-data-report.cfm

6 Frontier Economics Ltd. (2016). **The economic impacts of counterfeiting and piracy.** Report prepared for BASCAP and INTA.

7 Watson, J. (2016). **Safety and security in the Internet of Things.** Presentation by Professor Jeremy Watson, Engineering Systems, UCL; Director: PETRAS; Chief Scientist & Engineer, BRE; President of the IET at the Lloyd's Register Foundation 2016 Annual Conference. https://www.youtube.com/watch?v=cdtHZjL_5wk

8 Deshpande, A; Stewart, K; Lepetit, L & Gunashekar, S. (2017). **Distributed ledger technologies/blockchain: Challenges, opportunities and the prospects for standards.** British Standards Institution, London.

9 http://dictionary.cambridge.org

10 Hearn, M. (2016). **Corda - A distributed ledger.** Corda Technical White Paper.

11 Buterin, V. (2015). **On public and private blockchains.** Ethereum Blog, 7. https://blog.ethereum.org/category/crypto-renaissance-salon/

12 Rahimi, SK & Haug, FS. (2010). **Distributed database management systems: A practical approach.** John Wiley & Sons.

13 **How does Bitcoin work?** (nd). https://bitcoin.org/en/how-it-works

14 https://www.multichain.com/

15 http://www.agilitysciences.com/

16 **Trust, confidence and Verifiable Data Audit.** (nd). https://deepmind.com/blog/trust-confidence-verifiable-data-audit/

17 Merkle, RC. (1979). **Secrecy, authentication, and public-key systems.** PhD thesis, Stanford University.

18 Apostolaki, M; Zohar, A & Vanbever, L. (2017, May). **Hijacking Bitcoin: Routing attacks on cryptocurrencies.** In *Security and Privacy (SP), 2017 IEEE Symposium on* (pp. 375-392). IEEE.

19 Buterin, V. (2014). **A next-generation smart contract and decentralized application platform.** Ethereum Whitepaper. https://github.com/ethereum/wiki/wiki/White-Paper

20 Buterin, V. (2016). **Ethereum 2.0 Mauve Paper** https://cdn.hackaday.io/files/10879465447136/Mauve%20Paper%20Vitalik.pdf

21 http://dapps.ethercasts.com/

22 Delmolino, K; Arnett, M; Kosba, A; Miller, A & Shi, E. (2016). **Step by step towards creating a safe smart contract: Lessons and insights from a cryptocurrency lab.** In *International Conference on Financial Cryptography and Data Security* (pp. 79-94). Springer Berlin Heidelberg.

23 **About Hyperledger.** (nd). https://www.hyperledger.org/about

24 Brown, RG; Carlyle, J; Grigg, I & Hearn, M. (2016). **Corda: An introduction.** R3 CEV, August.

25 **IBM Blockchain based on Hyperledger Fabric from the Linux Foundation.** (nd). https://www.ibm.com/blockchain/hyperledger.html

26 Lloyd's Register Foundation. (2014). **Foresight review of big data: Towards data-centric engineering.** www.lrfoundation.org.uk/publications/bigdata.aspx

27 Lloyd's Register Foundation. (2015). **Foresight review of resilience engineering: Designing for the expected and unexpected.** www.lrfoundation.org.uk/publications/resilience-engineering.aspx

28 Greenspan, G. (22 November 2015). **Avoiding the pointless blockchain project.** MultiChain blog. https://www.multichain.com/blog/2015/11/avoiding-pointless-blockchain-project/

29 Finextra (9 December 2016). **Everledger secures the first bottle of wine on the blockchain.** https://www.finextra.com/pressarticle/67381/everledger-secures-the-first-bottle-of-wine-on-the-blockchain

30 Donnelly, J. (2 May 2016). **Everledger plans blockchain database to combat art fraud.** CoinDesk. https://www.coindesk.com/everledger-announces-partnership-vastari-combat-art-fraud/

31 San Pedro, L. (2017). **Join us in setting a new standard for trust in the coffee industry.** Provenance. https://www.provenance.org/news/movement/coffee/

32 **Sustainable development goal 16.** (nd). https://sustainabledevelopment.un.org/sdg16

33 https://aid.technology/

34 **About Smart ID.** (nd). https://www.deloitte.co.uk/smartid/

35 Hewlett Packard Enterprise. (2016). **Making manufacturers greener.** HPE International Material Data System. www.public.mdsystem.com

36 **Digital railway.** (nd). https://www.networkrail.co.uk/our-railway-upgrade-plan/digital-railway/

37 Gartner. (7 February 2017). **Gartner says 8.4 billion connected "things" will be in use in 2017, up 31 percent from 2016.** http://www.gartner.com/newsroom/id/3598917

38 Banafa, A. (2017). **IoT and blockchain convergence: Benefits and challenges.** *IEEE IoT Newsletter January 2017.* http://iot.ieee.org/newsletter/january-2017/iot-and-blockchain-convergence-benefits-and-challenges.html

39 PETRAS. **The internet of energy things: supporting peer-to-peer energy trading and demand side management through blockchains.** (P2P-IoET). Current PETRAS project. Lead: Prof. D Shipworth, UCL / Partners: Siemens, UKPN. https://www.petrashub.org/portfolio-item/the-internet-of-energy-things-p2p-ioet/

40 Antonopolous, M. (22 February 2017) **Blockchain for beginners.** Presentation at the Bloktex Event, Malaysia. https://youtu.be/i9nUMvpT2rM

41 Provenance. (15 July 2016). **From shore to plate: Tracking tuna on the blockchain.** https://www.provenance.org/tracking-tuna-on-the-blockchain

42 Gross, R. (16 May 2016). **Unveiling Blockchain's potential together: SAP Launches SAP Cloud Platform Blockchain Service.** SAP. http://news.sap.com/sapphire-now-sap-cloud-platform-blockchain-service/

43 Sculley, J. (18 Novermber 2014). **The most valuable lesson I learned from Steve Jobs.** https://www.entrepreneur.com/video/239801

44 Danezis, G & Meiklejohn, S. (2015). **Centrally banked cryptocurrencies.** *arXiv preprint arXiv:1505.06895.*

45 **Sawtooth introduction.** (nd). http://intelledger.github.io/0.8/introduction.html

46 **Intel® Software Guard Extensions (Intel® SGX).** (nd). https://software.intel.com/en-us/sgx

47 Sasson, EB et al. (2014, May). **Zerocash: Decentralized anonymous payments from bitcoin.** In *Security and Privacy (SP), 2014 IEEE Symposium on* (pp. 459-474). IEEE. http://zerocash-project.org/media/pdf/zerocash-extended-20140518.pdf

48 Goldwasser, S; Micali, S & Rackoff, C. (1985). **The knowledge complexity of interactive proof systems.** *Proceedings of the seventeenth annual ACM symposium on theory of computing*, pages 291{304. ACM, 1985.

49 Buterin, V. (15 January 2016). **Privacy on the Blockchain.** Ethereum Blog https://blog.ethereum.org/2016/01/15/privacy-on-the-blockchain/

50 Lehdonvirta, V. (21 November 2016). **The blockchain paradox: Why distributed ledger technologies may do little to transform the economy.** Oxford Internet Institute blog. https://www.oii.ox.ac.uk/blog/the-blockchain-paradox-why-distributed-ledger-technologies-may-do-little-to-transform-the-economy/

51 Del Castillo, M. (25 January 2017). **Microsoft unveils Project Manifest, a plan for Blockchain product tracking.** Coindesk. http://www.coindesk.com/microsoft-unveils-project-manifest-a-plan-for-product-tracking-via-blockchain/

52 Gil-Pulgar, J. (5 December 2016). **New developments in quantum computing impact Bitcoin.** Bitcoin News. https://news.bitcoin.com/bitcoin-ready-quantum-computing/

53 Jorgensen, MB. (20 September 2016). **How blockchain can resist the quantum computing security threat.** Ericsson blog. http://cloudblog.ericsson.com/how-blockchain-can-resist-the-quantum-computing-security-threat

54 Suichies, B. (21 December 2015). **Why Blockchain must die in 2016.** Medium. https://medium.com/@bsuichies/why-blockchain-must-die-in-2016-e992774c03b4

Further reading

Research projects

Applications of distributed ledger technology. EPSRC funding calls – Invitation for outline proposals, May 2016. https://www.epsrc.ac.uk/funding/calls/ledgermay2016/

Blockchain-empowered infrastructure for IoT (BlockIT). PETRAS project. Lead: W Hall, University of Southampton, UK. Partners: British Gas, DSTL. https://www.petrashub.org/projects-by-themes/

Blockchain technology for IoT in intelligent transportation systems (B-IoT). PETRAS project. Lead: M Huth, Imperial College London, UK. Partners: Ordinance Survey, Wallet. Services, Pinsent Masons, Telefonica, CISCO. https://www.petrashub.org/projects-by-themes/

Glass houses: Transparency and privacy in information economies. EP/N028104/1 Lead: S Meiklejohn, University College London, UK. http://gtr.rcuk.ac.uk/projects?ref=EP%2FN028104%2F1

Ox-Chain: Towards secure and trustworthy circular economies through distributed ledger technologies. R EP/N028198/1. Lead: C Speed, University of Edinburgh, UK. http://gtr.rcuk.ac.uk/projects?ref=EP%2FN028198%2F1

Project Novum: Distributed ledger technologies and structural change in financial and cultural services. Lead: V Lehdonvirta, University of Oxford, UK. https://www.oii.ox.ac.uk/research/projects/project-novum-distributed-ledger-technologies-and-structural-change-in-financial-and-cultural-services/

Websites

Coala.global. International multidisciplinary collaborative research and development initiative for blockchain technologies. http://coala.global/index.html

Ethereum Homestead documentation. http://www.ethdocs.org/en/latest/

Hyperledger Fabric documentation. http://hyperledger-fabric.readthedocs.io/en/master/

Ledger. A peer-reviewed scholarly journal. https://ledgerjournal.org/ojs/index.php/ledger

Articles and books

Al-Bassam, M; Sonnino, A; Bano, S; Hrycyszyn, D & Danezis, G. (2017). **Chainspace: A sharded smart contracts platform.** *arXiv preprint arXiv:1708.03778*.

Antonopoulos, AM. (2014). **Mastering Bitcoin: unlocking digital cryptocurrencies.** O'Reilly Media, Inc.

Atzei, N; Bartoletti, M & Cimoli, T. (2017, April). **A survey of attacks on Ethereum smart contracts (SoK).** In *International Conference on Principles of Security and Trust* (pp. 164-186). Springer, Berlin, Heidelberg.

Back, A. (2002). **Hashcash - a denial of service counter-measure.**

Bootle, J; Cerulli, A; Chaidos, P & Groth, J. (2015). **Efficient zero-knowledge proof systems.** In *Foundations of Security Analysis and Design* VIII (pp. 1-31). Springer, Cham.

Brown, RG; Carlyle, J; Grigg, I & Hearn, M. (2016). **Corda: An Introduction.** R3 CEV, August.

Chase, M & Meiklejohn, S. (2016). **Transparency overlays and applications.** In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security* (pp. 168-179). ACM.

Conner, S. (11 April 2017). **IC3RE announces partnership to explore convergence of blockchain and deep tech.** Imperial Centre for Cryptocurrency Research and Engineering (IC3RE) and OutlierVentures.io
http://www3.imperial.ac.uk/newsandeventspggrp/imperialcollege/centres/cryptocurrency/newssummary/news_19-4-2017-14-30-54

Ellis, JH. (1970). **The possibility of secure non-secret digital encryption.** *UK Communications Electronics Security Group*, 6.

Extance, A. (2015). **Bitcoin and beyond.** *Nature*, 526(7571), 21.

Gupta, V & ConsenSys LLC. (2017). **Building the hyperconnected future on blockchains.** Report from the World Government Summit 2017.
https://www.worldgovernmentsummit.org/annual-gathering/reports

Haber, S & Stornetta, WS. (1991). **How to time-stamp a digital document.** *Journal of Cryptology*, Vol 3, No. 2, pp. 99-111, 1991

Jogenfors, J. (2016). **Quantum bitcoin: An anonymous and distributed currency secured by the no-cloning theorem of quantum mechanics.** *arXiv preprint arXiv:1604.01383.*

Jorgensen, MB & Cohn, MB. (2016). **Industrialized blockchain and data integrity.** Ericsson. https://asset.zeqr.com/classFiles/2017/Apr/1491981429-58edd475b6393.pdf

Keshav, S. (2017). **Scalable blockchains for transactive energy.** Presentation at The Alan Turing Institute, London, 31 July 2017. http://blizzard.cs.uwaterloo.ca/iss4e/wp-content/uploads/2017/08/EnergyBlockchain.pptx

Kniesburges, S & Scheideler, C. (2011). **Hashed Patricia Trie: Efficient longest prefix matching in peer-to-peer systems.** In *WALCOM* (pp. 170-181).

Lamport, L; Shostak, R & Pease, M. (1982). **The Byzantine generals problem.** *ACM Transactions on Programming Languages and Systems (TOPLAS)*, 4(3), 382-401.

Laurie, B. (2011). **An efficient distributed currency.** *Practice*, 100.

Merkle, RC. (1980). **Protocols for public key cryptosystems.** In *Security and Privacy, 1980 IEEE Symposium on* (pp. 122-122). IEEE.

Mulligan, C. (nd). **Blockchain and digital transformation.** Presentation. Centre for Cryptocurrency Research and Engineering, Imperial College, London. http://www.imperial.ac.uk/media/imperial-college/research-and-innovation/thinkspace/public/1000_Catherine-Mulligan.pdf

Mulligan, C; Kenyon, T & Zylka, K. (4 April 2017). **The role of distributed ledgers in securing urban infrastructure.** Imperial College London blog. https://wwwf.imperial.ac.uk/blog/security-institute/2017/04/04/the-role-of-distributed-ledgers-in-securing-urban-infrastructure/

Narayanan, A; Bonneau, J; Felten, E; Miller, A & Goldfeder, S. (2016). **Bitcoin and cryptocurrency technologies: A comprehensive introduction.** Princeton University Press.

Von Neumann, J & Morgenstern, O. (2007). **Theory of games and economic behavior.** Princeton University Press.

Lloyd's Register Foundation

The Alan Turing Institute

Lloyd's Register Foundation
Report Series: No. 2017.4